IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

A

PATENT APPLICATION

Charles Calvin Byers
Mark Alan Lassig
Steven Mark Miller
William Brohmer Paulson
Carl Robert Posthuma

CASE 27-5-3-4-13

TITLE Method For Determining The Security Status Of Transmissions In A Telecommunications Network

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

NEW APPLICATION UNDER 37 CFR 1.53(b)

Enclosed are the following papers relating to the above-named application for patent:

Specification
4 Informal sheets of drawing(s)
1 Assignment with Cover Sheet
Declaration and Power of Attorney

CLAIMS AS FILED				
	NO. FILED	NO. EXTRA	RATE	CALCULATIONS
Total Claims	25 – 20 =	5	x $18 =	$90
Independent Claims	4 – 3 =	1	x $78 =	$78
Multiple Dependent Claim(s), if applicable			$260 =	$260
Basic Fee				$760
			TOTAL FEE:	$1188

Please file the application and charge **Lucent Technologies Deposit Account No. 12-2325** the amount of $1188, to cover the filing fee. Duplicate copies of this letter are enclosed. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 12-2325** as required to correct the error.

The Assistant Commissioner for Patents is hereby authorized to treat any concurrent or future reply, requiring a petition for extension of time under 37 CFR § 1.136 for its timely submission, as incorporating a petition for extension of time for the appropriate length of time if not submitted with the reply.

Please address all correspondence to **Docket Administrator (Room 3C-512), Lucent Technologies Inc., 600 Mountain Avenue, P. O. Box 636, Murray Hill, New Jersey 07974-0636.** However, telephone calls should be made to me at 630-979-0328.

Respectfully,

Mony R. Ghose
Reg. No. 38159
Attorney for Applicant(s)

Date: June 30, 1999

Lucent Technologies Inc.
600 Mountain Avenue
P. O. Box 636
Murray Hill, New Jersey 07974-0636

PT 13 10/98

"Express Mail" mailing label number EJ560395159US
Date of Deposit JUNE 30, 1999
I hereby certify that this application is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above, and is addressed to:
Assistant Commissioner for Patents - Washington, DC 20231
JUDITH A. SPOHN
(Printed name of person mailing paper or fee)
Judith A. Spohn
(Signature of person mailing paper or fee)

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Patent Application

Inventor	**Charles C. Byers** **Mark A. Lassig** **Steven M. Miller** **William B. Paulson** **Carl R. Posthuma**
Case	**27-5-3-4-13**
Serial No.	**Group Art Unit**
Filing Date	
Examiner	

Title **Method For Determining The Security Status Of Transmissions In A Telecommunications Network**

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

PRELIMINARY AMENDMENT

Please enter the following preliminary amendment to the above-identified application:

In the Specification:

On page 2, line 29, after "121," delete "139 and 177" and substitute therefor --131, 141, 151 and 161--.

REMARKS

This Preliminary Amendment is being submitted to correct a typographical error on page 2, line 29 which was discovered after the signing of the patent application.

Respectfully,

Charles C. Byers
Mark A. Lassig
Steven M. Miller
William B. Paulson
Carl R. Posthuma

By: Mony R. Ghose
Mony R. Ghose, Attorney
Reg. No. 38159
(630) 979-0328

Lucent Technologies Inc.
Date June 30, 1999

"Express Mail" mailing label number EJ560395159US
Date of Deposit JUNE 30, 1999
I hereby certify that this PRELIMINARY AMENDMENT is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above, and is addressed to: Assistant Commissioner for Patents - Washington, DC 20231
JUDITH A. SPOHN
(Printed name of person mailing paper or fee)
Judith A. Spohn
(Signature of person mailing paper or fee)

METHOD FOR DETERMINING THE SECURITY STATUS OF TRANSMISSIONS IN A TELECOMMUNICATIONS NETWORK

Technical Field:

This invention relates to telecommunications networks, and more particularly, to ascertaining information about and providing an indication of the security status of transmissions in such telecommunications networks.

Background of the Invention:

Modern day telecommunications networks are a web of a variety of nodes for delivering information from sender to recipient. In traditional public switched telephone networks (PSTNs), these nodes are circuit switched connections for relaying information along presumably secure, well-established routes. A relatively new phenomenon in telecommunications is the emergence of packet data networks. Transmission routes in packet data networks are dynamic and allow flexibility in information flow so that data is transmitted along paths most efficient for delivery. Indeed, the hallmark of the packet data network is its method of routing which ensures greater bandwidth for delivery of information.

An issue associated with all telecommunications transmissions, but more pronounced in packet data networks (due to the unpredictable nature of packet transmission routes), is the security of the node through which the information passes. This is because unauthorized interception of transmission is possible at many points along a route using relatively unsophisticated equipment. In some applications, such as military or corporate communications, a secure transmission is essential. With the increasing convergence of packet data and circuit switched networks, the likelihood of transmitting information via a network node which is subject to interception is significant. Therefore, traditional assumptions about the security of telecommunications networks, or the nodes contained therein, are no longer warranted.

Summary of the Invention:

It is recognized that most users of telecommunications services expect some degree of privacy when transmitting information across a network. There is currently a need for alerting users when a transmission is subject to interception due to its traversal of an insecure node in a telecommunications network.

This need is addressed and a technological advance is achieved in the telecommunications art by alerting senders or recipients whenever information has traversed

at least one insecure node in a telecommunications network. Upon receipt of the security status of the node, the parties may elect to continue communication or decline transmission. A node is considered insecure if it does not have the capability to send or receive private or encrypted information or passes through facilities not absolutely controlled by a network provider. Circuit switched transmissions are private but not usually encrypted.

More particularly, an originating system identifies a path to an end destination. If any portion of the path includes insecure links or nodes, the intended recipient of the transmission is alerted. The recipient may then elect to receive the call, using caution not to divulge confidential matters, or decline the call. Alternatively, each insecure node of the transmitting network issues a signal indicating its insecure status. The originating or terminating party can then elect to abort the transmission.

A variety of mechanisms for alerting the caller or recipient of the insecure nature of a call are available. For example, an insecure transmission may be denoted by a special message on the caller identification display, distinctive ringing, an audible message or a periodic audible tone. Advantageously, all parties involved in a transmission are actually informed of the security level of the network supporting the transmission so that intelligent decisions about content can be made.

Brief Description of the Drawings:

FIG. 1 is a simplified block diagram of a telecommunications network in which the method of the present invention may be practiced;

FIG. 2 is a call flow diagram illustrating steps performed in one embodiment of the present invention;

FIGs. 3 and 4 are call flow diagrams illustrating steps performed in second and third embodiments of the present invention.

Detailed Description:

FIG. 1 is a simplified block diagram of telecommunications network 100 comprising packet (or cell) network backbone 110 interconnected to internet service provider (ISP) access server 120, cable modem termination system 130, first voice gateway 140, second voice gateway 150 and mobile switching center 160 via links 121, 139 and 177, respectively. In this diagram, insecure links 121, 139 and 177 are denoted via dashed lines.

Among other components which are known in the art, packet network backbone 110 includes processor 111 for implementing data transmission procedures and security maintenance protocols as described herein. ISP access server 120 includes digital signal

processor 124 for security maintenance protocols as described below. ISP access server 120 serves personal computer 126 by established link 125. In this embodiment, personal computer 126 includes digital signal processing capability unit 128. Packet network backbone 110 is interconnected to cable modem termination system 130 via secure link 131. Cable modem termination system 130 includes digital signal processor 132 for security maintenance protocols.

Cable set top box 134 includes its own digital signal processor 136 and serves telephone 138. The cable set top box is interconnected to cable modem termination system 130 via insecure link 139. First voice gateway 140 is interconnected to PSTN 180 via link 143 while second voice gateway 150 is interconnected to the PSTN via link 153. The PSTN serves subscribers of traditional circuit switched network services. Voice gateways 140 and 150 allow these subscribers to communicate with subscribers of packet network backbone services or cable subscribers, such as those who use telephone 138. First voice gateway 140 and second voice gateway 150 are interconnected to the packet network backbone via secured links 141 and 151, respectively. It is well known that the network topology of circuit switched connections enhances security but packet transmissions are more subject to interception.

Mobile switching center 160, including digital signal processor 162, serves base station 170 by established link 165. Base station 170 serves mobile terminal 174 over insecure air interface 177. Mobile terminal 174 includes its own digital signal processor 176 for security maintenance protocols.

All secure nodes have digital signal processors capable of encryption or decryption of information. In this example, all digital signal processors have the ability to send information regarding node security status to other network nodes.

FIG. 2 illustrates the steps performed in telecommunications network 100 in accordance with one embodiment of the present invention. Although the example describes a voice call, those skilled in the art will recognize that any form of communication connection may be applied. The process begins in step 200 in which an originating system, such as cable set top box 134, receives dialed digits identifying a called party (e.g., the user served by personal computer 126). In step 202, the originating system establishes a call path to the called party. In this case, assume the call path comprises links 139, 131, 121 and 125.

In decision step 204, it is determined whether the call path includes insecure links. If the outcome of decision step 204 is a "NO" determination, the process continues to step 205

in which the call is processed to completion. If, as in this case, the outcome of decision step 204 is a "YES" determination, the process continues to step 206 in which the originating system determines if it has encryption capability and sends a query to the terminating system to determine if decryption capability exists at the end destination. In this example, the cable set top box does not have encryption capability. Therefore, it does not matter if the end destination has decryption capability. However, to illustrate this step, assume that the set top box issues a query to ISP access server 120 to determine whether personal computer 126 includes a digital signal processor 128 for decryption of a transmission. In this example, digital signal processor 128 is capable of decryption. If an originating system does not have encryption capability, it is likely to use the process described in FIG. 4 (i.e., finding a completely secure path).

The process continues to decision step 208 in which it is determined whether the system of the end destination can process an encrypted message. In this example, ISP access server 120 queries personal computer digital signal processor 128 to determine whether it has decryption capability. If the outcome of decision step 208 is a "NO" determination, the process continues to step 210 in which the originating system issues an insecure transmission warning to the caller using telephone 138. In decision step 212, the originating system determines if the caller wishes to continue the call. If the outcome of decision step 212 is a "NO" determination, the process ends in step 214. If the outcome of decision step 212 is a "YES" determination, the process continues to step 213 in which an insecure transmission warning is issued to the called party served by personal computer 126 prior to making the call connection. If the outcome of decision step 208 is a "YES" determination, the process continues to step 216 in which the originating system (if capable of doing so) sends an encrypted transmission to the called party via the established call path. In this example, the originating system cannot encrypt messages so the transmission is sent with a warning. In step 218, the called party receives the encrypted transmission and, if applicable, decryption software is applied. In step 220, the call is completed with normal processing after the received transmission is decrypted. Of course, if both originating and terminating systems have encryption capability, all transmissions between the parties are encrypted and secure.

FIG. 3 is a flow diagram illustrating the steps performed in telecommunications network 100 from the perspective of an insecure network node. FIG. 3 should be viewed in conjunction with FIG. 4.

The process begins in step 300 in which an originating system looks up a subscriber security profile for the caller and if the caller subscribes to enhanced security services, sends a transmission to an end destination with a request for security status of each node in the route from originating to termination systems. The request for a security status is appended to packet data and identifies the address of the originating system. Security status messages are returned to the originating system in accordance with a security maintenance protocol stored in the node. The security status protocol is based on customer-specific security profiles stored in the originating system processor or an external data base. Various parameters may be established based on subscriber features. For example, the customer may specify certain transmissions (e.g., transmissions after 5:00 p.m.) in which no security checks are required.

The process continues to step 302 in which an insecure node in the network receives the unencrypted transmission from the originating system. In decision step 304, the node determines if the transmission includes a security status request. If the outcome of decision step 304 is a "NO" determination, the process continues to step 305 in which normal procedures are undertaken to complete the transmission. If the outcome of decision step 304 is a "YES" determination, the process continues to step 306 in which the node sends a security alert message to the originating system and waits for further instructions from the system. Processing of security alert messages is described in FIG. 4.

In decision step 308, the node which sent the security alert message determines if the transmission should be continued based on instructions received from the originating system. If the outcome of decision step 308 is a "YES" determination, the process returns to step 305 in which normal procedures are used to complete the transmission. If the outcome of decision step 308 is a "NO" determination, the process ends in step 310 in which the transmission is abandoned and all applications are terminated.

FIG. 4 illustrates the steps performed in telecommunications network 100 from the perspective of an originating system.

The process begins in step 400 in which an originating system sends a transmission along a route traversing a packet data network. The transmission includes a request for security status confirmation. In decision step 402, the originating system determines if the transmission route is pre-established. If the outcome of decision step 402 is a "YES" determination, the originating system determines if the pre-established route is completely secure. If the outcome of decision step 404 is a "YES" determination, the process continues to step 406 in which normal transmission procedures occur. In some instances, a route which

was originally identified as secure becomes insecure due to last minute route changes (e.g., traversal of the world wide web for routing efficiency) or entry into another service provider's realm, such as a roaming mobile terminal. Thus, in some embodiments, the originating system monitors the transmission route for security alert signals so that the caller and called party can be notified if a previously secure route becomes insecure. If the outcome of decision step 402 is a "NO" determination, the process continues to step 408 in which the originating system waits for security status alert messages after sending the transmission. Processing of security status requests is described in FIG. 3.

In decision step 410, the originating system determines if any security alert messages are received. If the outcome of decision step 410 is a "NO" determination, the process continues to step 411 in which the originating system assumes the transmission has been completed without security compromises. If the outcome of decision step 410 is a "YES" determination, the process continues to step 412 in which the originating system responds to the received security alert message by sending an insecure transmission warning to the originator of the transmission and the proposed recipient of the transmission. The insecure message indication may take the form of an audible tone, audible message, a visual display or a query screen on a personal computer. Also, an audible tone may be periodically inserted throughout the call to remind the parties of the insecure nature of the connection.

In decision step 414, the originating party determines if either party wants to try another transmission route based on the insecure transmission warning. If the outcome of decision step 414 is a "YES" determination, the process continues to step 415 in which the originating system attempts to locate a secure transmission route. In decision step 416, the originating system determines if a secure transmission route is found. If the outcome of decision step 416 is a "YES" determination, the process returns to step 406. If the outcome of decision step 416 is a "NO" determination, the process continues to decision step 418 in which the originating system determines if parties want to continue transmission. If the outcome of decision step 418 is a "NO" determination, the process continues to step 419 in which the transmission is abandoned and the application is terminated. If the outcome of decision step 418 is a "YES" determination, the process returns to step 406.

The embodiments described above include customer premises equipment (such as telephones, fax machines or personal computers) with mechanisms for responding to security protocols. More particularly, the customer premises equipment is able to send signals indicating that a call or transmission should continue or be discontinued based on the security

level of the transmission. Advantageously, all embodiments allow all parties involved in a call or information exchange to ascertain the level of security associated with a communication prior to actual transmission. In this manner, the security of the exchange is enhanced by the knowledge of the security level associated with the call.

It is to be understood that the above description is only of one preferred embodiment of the invention. Numerous other arrangements may be devised by one skilled in the art without departing from the scope of the invention. The invention is thus limited only as defined in the accompanying claims.

What is claimed is:

1. A telecommunications network comprising:

an originating system connected to a terminating system via at least one other network element; and

a network element equipped with a processor for transmitting a message to the terminating system indicating that a transmission was received over an insecure link.

2. The telecommunications network of claim 1 further comprising the terminating system alerting a called station of the insecure nature of the transmission upon receipt of the insecure message.

3. A telecommunications network of claim 1 further comprising the originating system alerting a calling party of the insecure link.

4. A method for providing secure transmissions in a telecommunications network comprising the steps of:

establishing a route from a sender to a recipient;

determining whether at least a portion of the route includes an insecure link; and

providing an alert of the insecure nature of the transmission upon the determination that the route includes an insecure link.

5. The method of claim 4 further comprising the step of:

completing a call after the alert has been provided.

6. The method of claim 4 wherein providing an alert includes issuing a distinctive ring at the recipient's station.

7. The method of claim 4 wherein providing an alert includes issuing a message on an identification display.

8. The method of claim 4 further comprising the sender receiving an insecure link warning prior to connection to the recipient.

9. The method of claim 4 wherein the alert is provided to the sender.

10. The method of claim 4 wherein providing an alert includes providing an audible voice message.

11. The method of claim 4 wherein providing an alert includes using an audible tone.

12. The method of claims 10 or 11 wherein providing an alert includes providing a periodic alert.

13. The method of claim 4 further comprising:

issuing an alert when a previously secure route becomes insecure.

14. The method of claim 4 wherein providing an alert includes a query screen on a personal computer.

15. A method for processing a request for a telecommunications connection comprising the steps of:

receiving a request to establish a portion of a route between parties, the request including a security protocol;

determining whether the route would include an insecure link; and

upon a determination that an insecure link exists, sending a security alert message.

16. The method of claim 15 further comprising establishing a portion of a route without sending a security alert message.

17. The method of claim 15 further comprising sending a security status request.

18. A telecommunications system comprising:

means for interconnecting a caller to a called party; and

means for alerting the caller or called party when a call path is established using at least one insecure link.

19. The telecommunications system of claim 18 wherein the call path traverses a packet data network.

20. The telecommunications system of claim 18 further comprising means for determining whether an insecure link has been traversed.

21. The telecommunications system of claim 18 further comprising means for issuing insecure link alert signals to other elements in a telecommunications network.

22. The telecommunications system of claim 18 further comprising means for the caller and called party to hear insecure warning signals throughout the call.

23. The telecommunications system of claim 18 wherein the call path traverses a cell network.

24. The telecommunications system of claim 18 wherein the means for alerting is subject to parameters established for a particular subscriber.

Abstract of the Invention:

A method for determining the security level associated with transmissions in a telecommunications network includes means for alerting parties of the security status of the transmission. When a route interconnecting the parties includes an insecure link, an alert is provided so that the parties are aware of the insecure nature of the call before communications begin. Alternatively, the parties may elect to decline or alter content of the communications to preserve integrity.

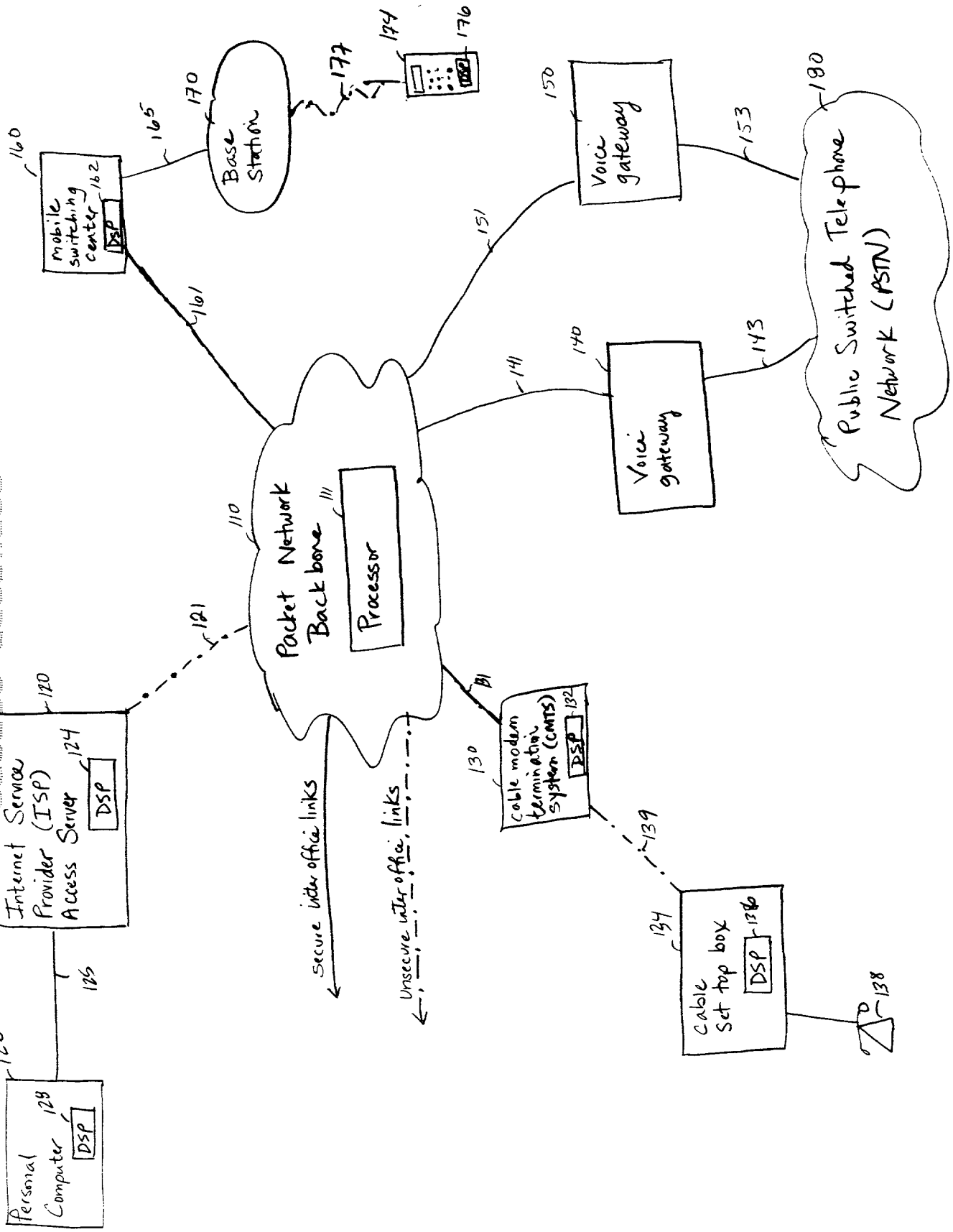
Packet Network Backbone
Processor
110
111
Internet Service Provider (ISP) Access Server
DSP
120
124
121
Personal Computer
DSP
126
129
125
Mobile switching center
DSP
160
162
161
Base Station
170
165
177
174
176
Voice gateway
150
151
153
Public Switched Telephone Network (PSTN)
180
Voice gateway
140
141
143
Cable modem termination system (CMTS)
DSP
130
132
131
139
Cable Set top box
DSP
134
136
138
Secure inter office links
Unsecure inter office links

Fig. 1

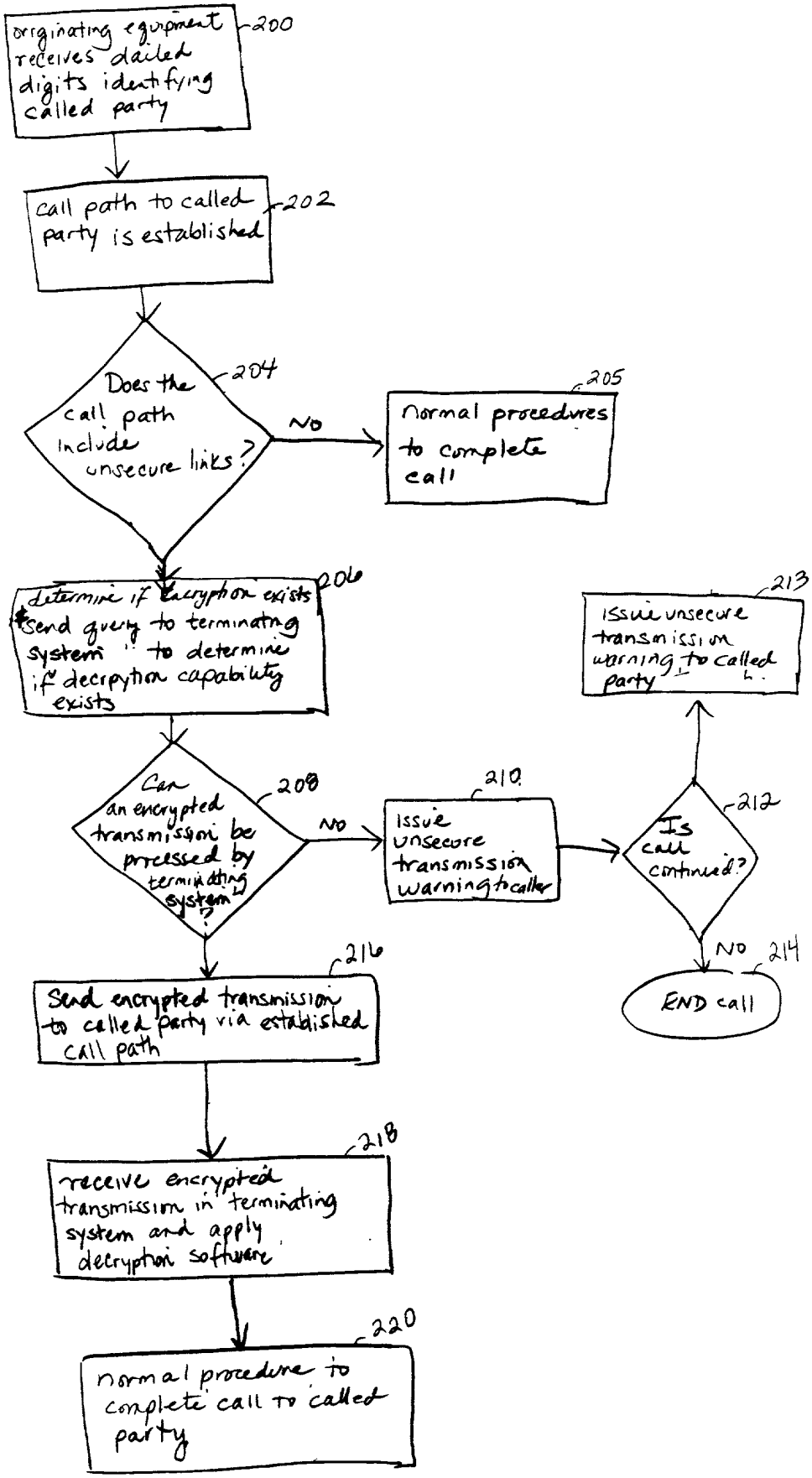
originating equipment receives dialed digits identifying called party
200
call path to called party is established
202
Does the call path include unsecure links?
204
No
normal procedures to complete call
205
determine if encryption exists send query to terminating system to determine if decryption capability exists
206
Can an encrypted transmission be processed by terminating system?
208
No
issue unsecure transmission warning to caller
210
Is call continued?
212
No
END call
214
issue unsecure transmission warning to called party
213
Send encrypted transmission to called party via established call path
216
receive encrypted transmission in terminating system and apply decryption software
218
normal procedure to complete call to called party
220

Fig. 2

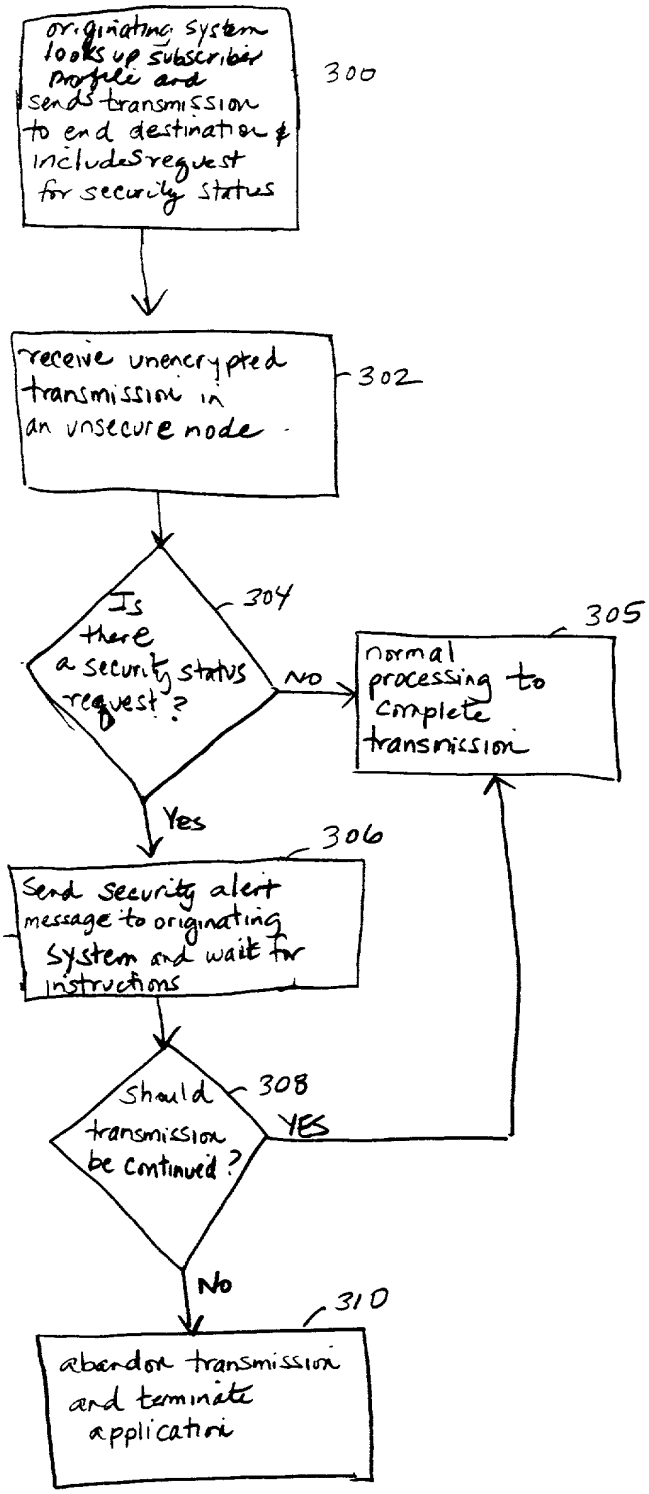
originating system looks up subscriber profile and sends transmission to end destination & includes request for security status
300
receive unencrypted transmission in an unsecure mode
302
Is there a security status request?
304
No
normal processing to complete transmission
305
Yes
Send security alert message to originating system and wait for instructions
306
Should transmission be continued?
308
YES
No
abandon transmission and terminate application
310

Fig. 3

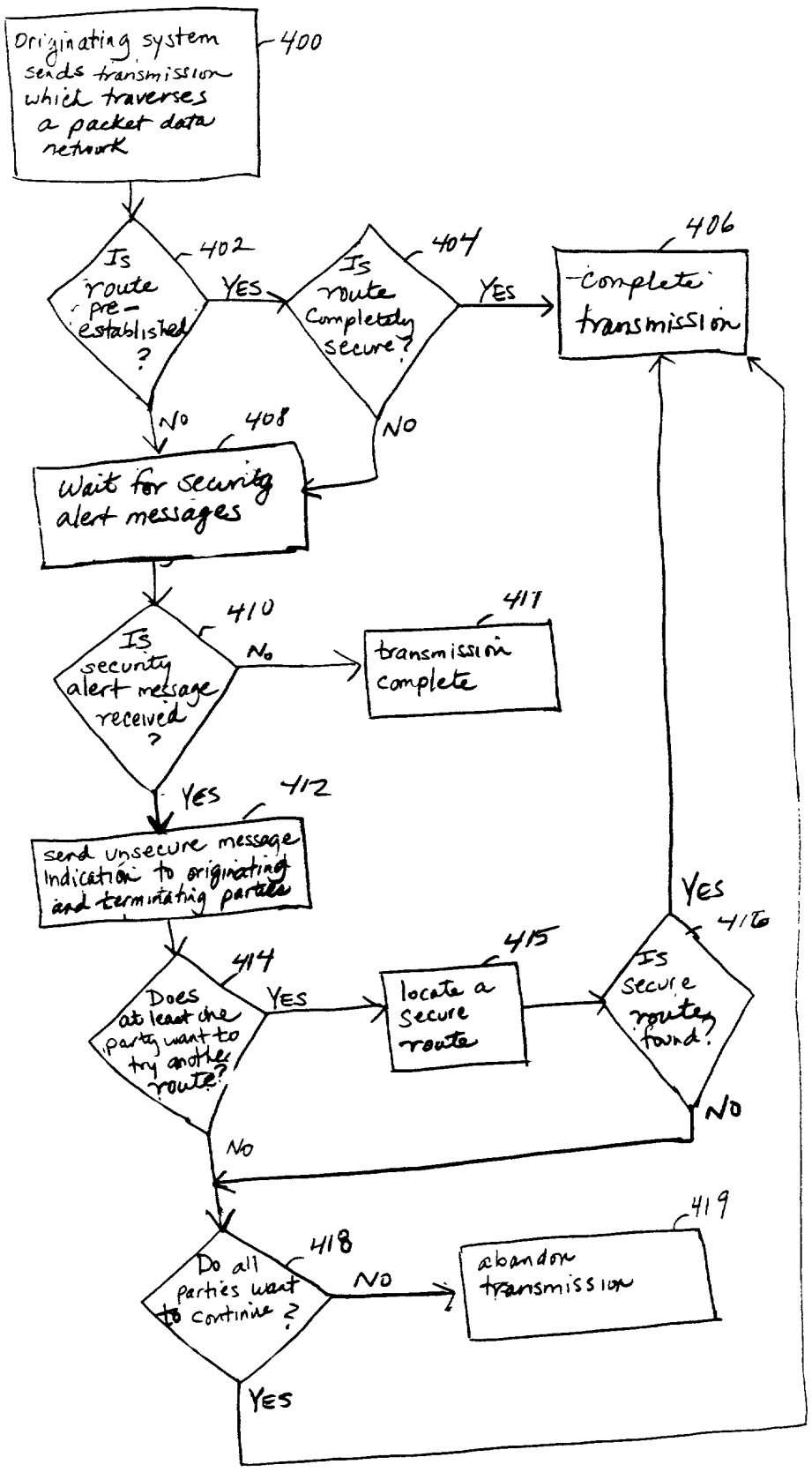
Originating system sends transmission which traverses a packet data network
400
Is route pre-established?
402
YES
Is route completely secure?
404
YES
Complete transmission
406
NO
NO
Wait for security alert messages
408
Is security alert message received?
410
No
transmission complete
411
YES
send unsecure message indication to originating and terminating parties
412
Does at least one party want to try another route?
414
YES
locate a secure route
415
Is secure route found?
416
YES
NO
NO
Do all parties want to continue?
418
NO
abandon transmission
419
YES

Fig. 4

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **Method For Determining The Security Status Of Transmissions In A Telecommunications Network** the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Thomas J. Bean	(Reg. No. P-44528)
Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
Craig J. Cox	(Reg. No. 39643)
Donald P. Dinella	(Reg. No. 39961)
Guy H. Eriksen	(Reg. No. 41736)
Martin I. Finston	(Reg. No. 31613)
James H. Fox	(Reg. No. 29379)
William S. Francos	(Reg. No. 38456)
Barry H. Freedman	(Reg. No. 26166)
Julio A. Garceran	(Reg. No. 37138)
Mony R. Ghose	(Reg. No. 38159)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
Stephen M. Gurey	(Reg. No. 27336)
John M. Harman	(Reg. No. 38173)
John W. Hayes	(Reg. No. 33900)
Michael B. Johannesen	(Reg. No. 35557)
Mark A. Kurisko	(Reg. No. 38944)
Irena Lager	(Reg. No. 39260)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Martin G. Meder	(Reg. No. 34674)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Joseph J. Opalach	(Reg. No. 36229)
Neil R. Ormos	(Reg. No. 35309)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Daniel J. Piotrowski	(Reg. No. 42079)
Gregory C. Ranieri	(Reg. No. 29695)
Scott J. Rittman	(Reg. No. 39010)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
Patricia A. Verlangieri	(Reg. No. 42201)
John P. Veschi	(Reg. No. 39058)
David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Jeffrey M. Weinick	(Reg. No. 36304)
Eli Weiss	(Reg. No. 17765)

Please address all correspondence to the Docket Administrator (Rm. 3C-512), Lucent Technologies Inc., 600 Mountain Avenue, P. O. Box 636, Murray Hill, New Jersey 07974-0636. Telephone calls should be made to Mony R. Ghose by dialing 630-979-0328.

Full name of 1st joint inventor: Charles Calvin Byers

Inventor's signature Charles Calvin Byers Date 6/29/99

Residence: Aurora, DuPage County, Illinois

Citizenship: United States of America

Post Office Address: 3203 Bremerton Lane
Aurora, Illinois 60504

Full name of 2nd joint inventor: Mark Alan Lassig

Inventor's signature Mark Alan Lassig Date 6/29/99

Residence: Naperville, DuPage County, Illinois

Citizenship: United States of America

Post Office Address: 1563 Selby Road
Naperville, Illinois 60563

Full name of 3rd joint inventor: Steven Mark Miller

Inventor's signature Steven Mark Miller Date 6-29-99

Residence: Batavia, Kane County, Illinois

Citizenship: United States of America

Post Office Address: 235 North Lincoln
Batavia, Illinois 60510

Full name of 4th joint inventor: William Brohmer Paulson

Inventor's signature *William Brohmer Paulson* Date 6/29/99

Residence: Naperville, DuPage County, Illinois

Citizenship: United States of America

Post Office Address: 5S371 Radcliff Road
Naperville, Illinois 60563

Full name of 5th joint inventor: Carl Robert Posthuma

Inventor's signature *Carl Robert Posthuma* Date 6/30/99

Residence: Wheaton, DuPage County, Illinois

Citizenship: United States of America

Post Office Address: 1309 Lowden Avenue
Wheaton, Illinois 60187